REMARKS/ARGUMENTS

In the Office Action mailed November 25, 2009, claims 1-13 were rejected. In response, Applicant hereby requests reconsideration of the application in view of the below-provided remarks. No claims are amended, added, or canceled.

Claim Rejections under 35 U.S.C. 103

Claims 1-13 were rejected based on one or more cited references. The cited reference(s) relied on in these rejections include:

Coron et al. ("Resistance Against Differential Power Analysis for Elliptic Curve Cryptosystems," 1999, pages 1-11, hereinafter Coron)

Lauter et al. (U.S. Pat. No. 7,043,015, hereinafter Lauter)

Lange ("Weighted Coordinates on Genus 2 Hyperelliptic Curves," October 11, 2002, pages 1-20, hereinafter Lange)

Okeya et al. (U.S. Pat. Pub. No. 2003/0059042, hereinafter Okeya)

Joye et al. ("Protections Against Differential Analysis for Elliptic Curve Cryptography," Springer-Verlag, 2001, pages 1-15, hereinafter Joye)

In particular, claims 1-4, 7, 8, and 10 were rejected under 35 U.S.C. 103(a) as being unpatentable over Coron in view of Lauter. Claims 1 and 8 were also separately rejected under 35 U.S.C. 103(a) as being unpatentable over Joye in view of Lauter. Claims 5, 6, and 11-13 were rejected under 35 U.S.C. 103(a) as being unpatentable over Coron in view of Lauter and in view of Lange. Claim 9 was rejected under 35 U.S.C. 103(a) as being unpatentable over Coron in view of Lauter and in view of Okeya. However, Applicant respectfully submits that these claims are patentable over Coron, Lauter, Lange, Okeya, and Joye for the reasons provided below.

Independent Claim 1

Claim 1 is patentable over the separate combinations of 1) Coron and Lauter, and 2) Joye and Lauter. Specifically, claim 1 is patentable over the proposed combination of

Coron and Lauter because the reasoning in the Office Action is not rational and, hence, is insufficient to establish a *prima facie* case of obviousness. Similarly, claim 1 is separately patentable over the proposed combination of Joye and Lauter because the Office Action does not present articulated reasoning to address the proposed combination of references and, hence, is insufficient to establish a *prima facie* case of obviousness. For reference, claim 1 recites:

> A method for defence against an attack made by means of differential power analysis, the method comprising:
>
> randomizing at least one factor in at least one hyperelliptic public key cryptosystem, which is given by at least one hyperelliptic curve of any genus over a finite field in a first group, where the hyperelliptic curve is given by at least one coefficient, wherein the factor is selected from the group consisting of:
>
> the hyperelliptic curve; and
>
> at least one element of the first group.

In order to establish a *prima facie* rejection of a claim under 35 U.S.C. 103, the Office Action must present a clear articulation of the reason why the claimed invention would have been obvious. MPEP 2142 (citing *KSR International Co. v. Teleflex Inc.*, 550 U.S. 398 (2007)). The analysis must be made explicit. Id. Additionally, rejections based on obviousness cannot be sustained by mere conclusory statements; instead there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness. Id.

Thus, there are at least three criteria that must be satisfied in order to establish a *prima facie* case of obviousness:

1) The rejection must include a conclusion that the claimed invention would have been obvious.
2) The rejection must include articulated reasoning to support the asserted conclusion of obviousness.
3) The articulated reasoning must be based on some rational underpinning.

In regard to the rejection of the claim based on the proposed combination of Coron and Lauter, the reasoning presented in the Office Action is not rational and, hence, is insufficient to establish a *prima facie* case of obviousness. In regard to the rejection of the claim based on the proposed combination of Joye and Lauter, the Office Action does not present articulated reasoning to address the proposed combination of references and, hence, is insufficient to establish a *prima facie* case of obviousness.

1. The articulated reasoning presented in the Office Action in support of the rejection based on Coron and Lauter lacks a rational underpinning.

While the Office Action appears to assert a conclusion of obviousness and articulated reasoning in support of the rejection based on the proposed combination of Coron and Lauter, the articulated reasoning is not based on a rational underpinning. Specifically, the articulated reasoning lacks a rational underpinning because the reasoning presented in the Office Action is not related to the proposed combination of teachings.

In support of the proposed combination of cited references, the articulated reasoning in the Office Action states:

> Coron does not explicitly disclose a hyperelliptic public cryptosystem. Lauter in analogous art, however, discloses a hyperelliptic public cryptosystem. (col. 4, line 1 –col. 5, line 18) Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system disclosed by Coron with Lauter in order to provide advantage of improved security while requiring shorter key lengths. (col. 2, lines 15-35; Lauter)
>
> Office Action, 11/25/09, page 3 (sic all) (emphasis added).

For a proper understanding of the basis for this reasoning, it should be noted that the cited portion of Lauter states:

> New curve-based cryptography techniques have recently been employed to allow software manufacturers to appreciably reduce the incidence of unauthorized copying of software products. For example, product IDs have been generated using elliptic curve cryptography techniques. The resulting product IDs provide improved security. Moreover, such IDs can be configured such that the user is not required to

> input too many characters. So far, the curve-based techniques have been based on curves with genus greater than or equal to two.
>
> It would be beneficial to be able to utilize higher genus curves, e.g., hyperelliptic curves with genus greater than or equal to two. Doing so will likely further improve security. Moreover, it would be beneficial for the resulting information (data) to have a size that is suitable for use as a short signature, product ID, and/or the like. Consequently, for this and other reasons there is a need for methods and apparati that provide for compression of the resulting information. In curve-based cryptosystems, for example, compressing the point information can significantly reduce the amount of data within the resulting compressed format.
>
> Lauter, col. 2, lines 15-24 (emphasis added).

While Lauter describes the ability to improve security and use shorter key lengths, it should be noted that these benefits are not a result of combining hyperelliptic and elliptic techniques. Rather, the advantages stated in Lauter are apparently for hyperelliptic or elliptic techniques relative to a conventional RSA (Rivest-Shamir-Adleman) method conventionally used for public/private key cryptology. See, Lauter, col. 1, line 41, through col. 2, lines 14.

Specifically, the Examiner asserts that an elliptic public key cryptosystem could be modified to use a hyperelliptic public key cryptosystem "in order to provide advantage of improved security while requiring shorter key lengths." However, the stated advantage comes from the secondary reference and specifically refers to the advantages of an elliptic curve cryptography technique compared with a conventional RSA (Rivest-Shamir-Adleman) method, which does not appear to be an elliptic or hyperelliptic technique. Thus, the stated advantage is not related to the proposed modification using the hyperelliptic technique within an elliptic system. In other words, even if the hyperelliptic or elliptic techniques described in Lauter may be used to improve security or use shorter key lengths compared with the RSA method, there is no description in Lauter of using a hyperelliptic technique in an elliptic system in order to achieve the stated advantages of improved security while requiring shorter key lengths. Therefore, the reasoning presented in the Office Action is not rational because it is based on advantages over the conventional RSA method, but is not related to any type of combination of hyperelliptic and elliptic techniques or systems.

For the reasons presented above, the articulated reasoning presented in support of the proposed combination of Coron and Lauter lacks a rational underpinning because the asserted reasoning is not related to a combination of hyperelliptic and elliptic techniques or systems. Consequently, the Office Action does not establish a *prima facie* case of obviousness because the articulated reasoning in the Office Action lacks a rational underpinning. Accordingly, Applicant respectfully asserts the rejection of claim 1 is improper because the Office Action does not establish a *prima facie* case of obviousness.

2. The rejection based on the combination of Joye and Lauter is not supported by a conclusion of obviousness and articulated reasoning to address the proposed combination.

While the Office Action asserts a rejection based on the proposed combination of Joye and Lauter, the rejection is not supported by any type of conclusion of obviousness or articulated reasoning related to the combination of Joye and Lauter. Rather, the rejection merely asserts certain teachings of Joye, without discussing any of the teachings of Lauter. Moreover, it appears that the asserted teachings of Joye are merely recitals from the last Office Action, because the asserted teachings of Joye address the language of the claim prior to the previous amendment.

It appears that the Examiner intended to rely on some of the teachings of Lauter to remedy the corresponding lack of teaching in Joye. However, there is no articulated reasoning to explain this omission. Given that there is no articulated reasoning, there is also no conclusion that it might have been obvious to combine teachings of Lauter with the teachings of Joye. In the absence of articulated reasoning and a conclusion of obviousness, Applicant respectfully submits that the assertions in the Office Action are not sufficient to establish a *prima facie* rejection. Accordingly, Applicant respectfully submits that the rejection of claim 1 under 35 U.S.C. 103(a) based on the proposed combination of Joye and Lauter should be withdrawn because the Office Action fails to establish a *prima facie* rejection for the proposed combination of cited references.

Independent Claim 8

Applicant respectfully asserts independent claim 8 is patentable over the proposed combinations of cited references at least for similar reasons to those stated above in regard to the rejections of independent claim 1. Claim 8 recites subject matter which is similar to the subject matter of claim 1 discussed above. Although the language of this claim differs from the language of claim 1, and the scope of each claim should be interpreted independently of other claims, Applicant respectfully asserts that the remarks provided above in regard to the rejection of claim 1 also apply to the rejection of claim 8.

Dependent Claims

Claims 2-7 and 9-13 depend from and incorporate all of the limitations of the corresponding independent claims 1 and 8. Applicant respectfully asserts claims 2-7 and 9-13 are allowable based on allowable base claims. Additionally, each of claims 2-7 and 9-13 may be allowable for further reasons.

CONCLUSION

Applicant respectfully requests reconsideration of the claims in view of the remarks made herein. A notice of allowance is earnestly solicited.

At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account **50-4019** pursuant to 37 C.F.R. 1.25. Additionally, please charge any fees to Deposit Account **50-4019** under 37 C.F.R. 1.16, 1.17, 1.19, 1.20 and 1.21.

Respectfully submitted,

/mark a. wilson/

Date: January 25, 2010

Mark A. Wilson
Reg. No. 43,994

Wilson & Ham
PMB: 348
2530 Berryessa Road
San Jose, CA 95132
Phone: (925) 249-1300
Fax: (925) 249-0111